NIAC Working Group on Internet Hardening

Interim Progress Report

George Conrades, Chairman and CEO - Akamai Technologies

Presented by

Andy Ellis, Director of Information Security - Akamai Technologies

13 July 2004

Agenda

- Background
- Methodology
- Challenges
- Recommendation Areas
- Next Steps

Background

- July 2003 meeting, President Bush asks NIAC what can be done to harden the Internet
- NIAC establishes a working group to address the challenge of Internet Hardening

Mission/Objectives

- Develop guidance based on best practices in Internet systems management
  - Infrastructure advice aimed at network operators
  - Customer environment advice aimed at end users and enterprise networks
- Evaluate long term technologies to improve the environment
- Derive policy recommendations for President Bush based on developed guidance
  - Government internal policies to increase security on government networks
  - Policies to encourage private sector security improvements

Methodology

- Created two study groups
  - Infrastructure protection
  - Customer environment
- Meeting weekly for duration of working group
  - Assessing state of "best practices" published by other organizations
  - Evaluated proposals and recommendations from other organizations

Study Group Participants

- George Conrades, Akamai
- Bora Akyol, Cisco
- Pete Allor, ISS
- Al Berkeley, Community of Science
- Matt Bishop, UCDavis
- Vint Cerf, MCI
- Steve Crocker, ICANN
- John Clarke, USCERT
- Richard Clarke, GoodHarbor Consulting
- Sean Convery, Cisco
- Andy Ellis, Akamai
- John Faherty, DHS
- Noam Freedman, Akamai
- Peg Grayson, V-One
- Barry Greene, Cisco
- Matt Korn, AOL
- Deb Miller, V-One
- Bob Mahoney, Zanshin Security
- Gerry Macdonald, AOL
- Paul Nicholas, EOP
- Mike Petry, MCI
- Jeff Schiller, MIT
- Howard Schmidt, eBay
- Marty Schulman, Juniper
- Paul Vixie, ISC
- Ken Watson, Cisco
- Nancy Wong, DHS
- Lee Zeichner, GMU

Challenges

- Distributed Denial of Service
  - The availability of easily compromised computers on the Internet provides attackers with potent weapons against Internet-connected systems
- Infrastructure Protocol Security
  - Technologies not designed to prevent false control messages, but Best Current Practices sufficient for now
  - For the long term, moving to more secure protocols may be required

Recommendation Areas

- Education and awareness
  - End-user system security
  - Corporate security
- Research
  - New technologies
  - Investigation of secure protocol versions
- Empowerment
  - ISPs to act against aggressors
  - Law enforcement to focus on attackers

Education and awareness

- Develop academic curricula targeted at security needs.
- Target, via mass media, end-users on Internet security requirements.
- Corporate information security—board level issue.

Research and Development

- Investigation of secure protocol versions
  - Exploration of costs and benefits; implementation schemes; new, more secure core technologies
- Advanced security management technologies, including:
  - Scalable tools for network analysis
- Security governance issues
  - Understanding factors relating to adoption of best practices
  - Security ROI business case studies

Empowerment

- Investigate methods for ISPs to provide security controls.
- Investigate barriers to law enforcement prosecution of cyber crimes.

Next Steps

- Finalize draft report for the NIAC
- Submit report to NIAC for review